

REMARKS

Claims 1-33 are presented for examination, with Claims 1, 10, 20, 25, and 30-33 being in independent form. Favorable reconsideration is requested.

The Office Action asserts that no certified copy of the Japanese priority document has been received. It is noted that a certified copy of the priority document was filed on August 27, 2001; however, due to a typographical error, that filing was directed to an incorrect Application number. Specifically, that filing was erroneously directed to Application No. 09/730,387. Attached is a copy of a PAIR printout for Application No. 09/730,387 showing that the certified copy for this application was received by the Patent and Trademark Office in that application on August 27, 2001. (The PAIR printout for Application No. 09/730,387 also shows that the proper certified copy of the priority document for that application was received by the PTO on June 18, 2001.) Accordingly, Applicants respectfully request that the certified copy of the priority document for this application, which was erroneously filed in Application No. 09/730,387, be removed from that file and placed in this file. Acknowledgment of the claim for foreign priority and the receipt of the certified copy in this application are respectfully requested.

Claims 1-3, 6-8, 10-14, 16, 17, 20, 21, 25, and 27 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,341,425 to Wasilewski et al. Claims 4, 5, 9, 15, 18, 19, 22-24, and 28-33 were rejected under 35 U.S.C. § 103(a) as being obvious from Wasilewski in view of U.S. Patent 5,319,705 to Halter et al.

Claim 1 is directed to a data processing apparatus including reception means, first encryption means, generating means, multiplexing means, and transmitting means. The reception means receives a plurality of transmitting requests of object data,

and the first encryption means encrypts at least a predetermined portion of the object data using first key data to produce encrypted object data. The generating means generates seed information which allows the first key data to be obtained therefrom, the seed information being generated after the reception means receives the transmitting requests. The multiplexing means multiplexes the plurality of object data and the encrypted object data to generate a data stream. The transmitting means individually transmits the seed information and the data stream, the seed information being transmitted after the reception means receives the transmitting requests.

Among other notable features of Claim 1, transmitting requests are received and then encrypted object data and seed information are individually transmitted. The seed information is generated after the transmitting requests are received, and allows first key data used to produce the encrypted object data to be obtained therefrom.

By virtue of the features of Claim 1, it can be easier to assure security than by transmitting a key itself which is used for encryption, or transmitting a key and seed information together with encrypted data. Also, by virtue of the features of Claim 1, security can be maintained at a reproducing side without the necessity to safely keep the seed information, since the seed information is generated to be transmitted after receiving the transmitting requests.

Wasilewski et al., as understood by Applicants, relates to encrypting data at a plurality of data transmission sites for transmission to a reception site. A set of data is encrypted at each of a plurality N of transmission sites for transmission to and subsequent decryption at at least one reception site. Each of the N transmission sites is provided with a broadcast key unique to that transmission site and a system key that is the same for all

transmission sites. At each transmission site, the system key and the broadcast key unique to that transmission site are convolved in a predetermined manner to generate a unique data encryption key for that transmission site. At each transmission site, a set of data is then encrypted with the unique data encryption key generated at that site. The sets of data uniquely encrypted at each transmission site are then transmitted to the reception site. There is stored, in a memory at the reception site, the system key and each of the broadcast keys to enable a selected one of the encrypted sets of data to be decrypted at the reception site. (See column 3, cited in the Office Action, and Figs. 2-5.)

The Office Action at page 2 asserts that Wasilewski et al. teaches seed information, and cites “pk program key, system key/Sk, broadcast key/Bk, col. 3, lines 12 et seq.)”. Applicants respectfully disagree with this assertion, and note that the terms of Claim 1 specify “generating means for generating seed information which allows said first key data to be obtained therefrom, wherein said seed information is generated after said reception means receives the transmitting requests.” Thus, the apparatus of Claim 1 generates seed information *after* transmitting requests are received.

The system and broadcast keys of Wasilewski et al. are provided initially on both the transmission and reception sides, and there is no teaching or suggestion in that patent that they are provided after transmitting requests are received. Specifically, Wasilewski et al. states at column 3, in the portion cited by the Examiner:

Each of the N transmission sites is provided with a broadcast key unique to that transmission site and a system key that is the same for all transmission sites... There is stored, in a memory at the reception site, the system key and each of the broadcast keys to enable a selected one of the encrypted sets of data to be decrypted at the reception site.

Furthermore, there is no teaching or suggestion in Wasilewski et al. that the program key (which is a key, e.g., reference numeral 106 of Fig. 3) is generated after transmitting requests are received. Wasilewski et al. merely states:

As shown in Fig. 3, the exemplary programmer site 100 has an encryptor 104 for encrypting the program data 102 at that site. Encryptor 104 encrypts the program data 102 with a locally generated "program key" 106. Encryption of a program, data by a "programmer" prevents unauthorized access to that programmer's data. (See column 9, lines 30-35.)

The Office Action states at page 2 that:

The data transmission sites/reception means receive a plurality of request for programs, services, and/or pay per view events from users or subscribers or television system. It then transmits specific program information (pk, and program data) back to the requestors in the form of a seed. This seed is used to encrypt and decrypt data for transmission security, see figure 3, and column 9, lines 20 et seq.

However, there is no teaching or suggestion in Wasilewski et al. that the so-called "seed" as used in the above paragraph is generated after requests for programs or services are received.

Additionally, the apparatus of Claim 1 transmits encrypted object data and seed information individually. In this regard, Applicants note that Wasilewski states, at column 9, lines 50-56:

A preferable method of supplying remote locations with the necessary program keys is to multiplex the program keys with the data those keys were used to encrypt and then to transmit the multiplexed program keys and encrypted program data to the remote locations.

Therefore, in Wasilewski et al., the program key is multiplexed with the encrypted program data and is transmitted together with the encrypted data. As such, it is submitted that Wasilewski et al. does not teach or suggest individually transmitting encrypted object data and seed information.

Nothing has been found in Wasilewski that would teach or suggest that (1) transmitting requests are received and then encrypted object data and seed information, which allows first key data used to produce the encrypted object data to be obtained therefrom, are individually transmitted, and (2) the seed information is generated to be transmitted after receiving the transmitting requests, as recited in Claim 1.

Accordingly, Claim 1 is seen to be clearly allowable over Wasilewski et al.

Independent Claims 10, 20, and 25 recite features similar in respect of the foregoing arguments to those of Claim 1 discussed above, and therefore are also believed to be patentable over Wasilewski et al. for at least the reasons discussed above.

Independent Claims 30-33 also recite features similar in many respects to those discussed above with respect to Claim 1. Moreover, nothing has been found in Halter et al. that would remedy the deficiencies of Wasilewski et al., discussed above in connection with Claim 1. Accordingly, Claims 30-33 are believed to be patentable over Wasilewski et al. and Halter et al., whether considered either separately or in any permissible combination (if any).

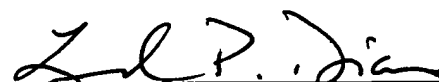
A review of the other art of record has failed to reveal anything which, in Applicants' opinion, would remedy the deficiencies of the art discussed above, as references against the independent claims herein. Those claims are therefore believed patentable over the art of record.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing remarks, Applicants respectfully request favorable reconsideration and early passage to issue of the present application.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "L. P. Diana", is written over a horizontal line.

Leonard P. Diana
Attorney for Applicants
Registration No.: 29,296

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

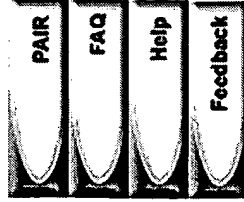


United States Patent and Trademark Office

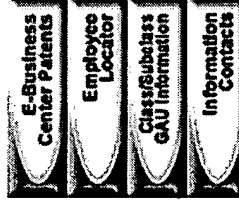
Home | Site Index | Search | FAQ | Glossary | Guides | Contacts | eBusiness | eBiz alerts | News | Help



PATENT APPLICATION INFORMATION RETRIEVAL



Other Links



Printer Friendly Version

Search results as of: 12-3-2005::22:10:2 E.T.

Search results for application number: 09730,387			
Application Number:	09730,387	Customer Number:	5514
Filing or 371(c) Date:	12-06-2000	Status:	Patented Case
Application Type:	Utility	Status Date:	01-15-2004
Examiner Name:	BAYAT, ALI	Location:	FILE REPOSITORY (FRANCONIA)
Group Art Unit:	2625	Location Date:	08-16-2004
Confirmation Number:	7427	Earliest Publication No:	US 2001-0051006 A1
Attorney Docket Number:	35.G2689	Earliest Publication Date:	12-13-2001
Class/ Sub-Class:	382/262	Patent Number:	6,687,413
First Named Inventor:	Akihiko Yushiya, Tokyo, (JP)	Issue Date of Patent:	02-03-2004
Title Of Invention: SIGNAL PROCESSING APPARATUS			

Select Search Option

Assignments Display References Foreign Priority Image File Wrapper Maintenance Fees - Retrieve fees to pay Maintenance Fees - View payment windows	<input type="button" value="Search"/>
---	---------------------------------------

Maintenance Fees Available: Mon-Fri 5:30 AM to Midnight, Sat-Sun-Hol. 7:30 AM to 8:00 PM E.T.

File History	
Date	Contents Description

02-03-2004	Recordation of Patent Grant Mailed
01-15-2004	Issue Notification Mailed
02-03-2004	Patent Issue Date Used in PTA Calculation
11-17-2003	Receipt into Pubs
11-13-2003	Application Is Considered Ready for Issue
09-09-2003	Correction - Oath or Declaration NOT Required
10-06-2003	Issue Fee Payment Verified
12-06-2000	Workflow - Drawings Finished
12-06-2000	Workflow - Drawings Matched with File at Contractor
10-30-2003	Receipt into Pubs
10-06-2003	Issue Fee Payment Received
09-12-2003	Workflow - File Sent to Contractor
09-11-2003	Receipt into Pubs
09-10-2003	Dispatch to Publications
09-09-2003	Mail Notice of Allowance
09-09-2003	Mail Oath of Declaration Required
09-08-2003	Oath or Declaration Required
09-08-2003	Notice of Allowance Data Verification Completed
08-06-2003	Case Docketed to Examiner in GAU
04-15-2003	Case Docketed to Examiner in GAU
03-27-2001	Request for Foreign Priority (Priority Papers May Be Included)
06-18-2001	Request for Foreign Priority (Priority Papers May Be Included)
05-14-2001	Information Disclosure Statement (IDS) Filed
05-13-2001	Case Docketed to Examiner in GAU
04-06-2001	IFW Scan & PACR Auto Security Review
01-17-2001	Application Dispatched from OIPE
01-11-2001	Correspondence Address Change
12-06-2000	Initial Exam Team nn

| HOME | INDEX | SEARCH | eBUSINESS | CONTACT US | PRIVACY STATEMENT